

UNITED STATES DISTRICT COURT

for the
Southern District of Texas

Sealed

Public and unofficial staff access
to this instrument are
prohibited by court order.

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

CERTAIN MICROSOFT EXCHANGE SERVERS
INFECTED WITH WEB SHELLS

Case No. 4:21mj 755

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the _____ District of _____ Multiple
(identify the person or describe the property to be searched and give its location):

See Attachment "A"

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment "B"

YOU ARE COMMANDED to execute this warrant on or before _____ (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to _____
Honorable Peter Bray
(United States Magistrate Judge)

☒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized (check the appropriate box)

☒ for 30 days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued:

4/9/21 @ 4:13 pm

Judge's signature

City and state:

Houston, Texas

Peter Bray, United States Magistrate Judge

Printed name and title

Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title

ATTACHMENT A
PROPERTY TO BE SEARCHED

This warrant applies to Microsoft Exchange Servers located in the United States onto which are installed web shells, identified by the shell paths listed below:

https://[REDACTED]/aspnet_client/system_web/[REDACTED].aspx

https://[REDACTED]/aspnet_client/system_web/[REDACTED].aspx

https://[REDACTED]/aspnet_client/system_web/[REDACTED].aspx

https://[REDACTED]/aspnet_client/system_web/[REDACTED].aspx

https://[REDACTED]/aspnet_client/system_web/[REDACTED].aspx

https://[REDACTED]/aspnet_client/system_web/[REDACTED].aspx

https://[REDACTED]/aspnet_client/system_web/[REDACTED].aspx

https://[REDACTED]/aspnet_client/system_web/[REDACTED].aspx

https://[REDACTED]/aspnet_client/system_web/[REDACTED].aspx

https://[REDACTED]/aspnet_client/system_web/[REDACTED].aspx

https://[REDACTED]/aspnet_client/system_web/[REDACTED].aspx

https://[REDACTED]/aspnet_client/system_web/[REDACTED].aspx

https://[REDACTED]/aspnet_client/system_web/[REDACTED].aspx

https://[REDACTED]/aspnet_client/system_web/[REDACTED].aspx

https://[REDACTED]/aspnet_client/system_web/[REDACTED].aspx

https://[REDACTED]/aspnet_client/system_web/[REDACTED].aspx

https://[REDACTED]/aspnet_client/system_web/[REDACTED].aspx

https://[REDACTED]/aspnet_client/system_web/[REDACTED].aspx

https://[REDACTED]/aspnet_client/system_web/[REDACTED].aspx

https://[REDACTED]/aspnet_client/system_web/[REDACTED].aspx

**Remaining pages
of Attachment A
are redacted in
their entirety**

ATTACHMENT B
PARTICULAR THINGS TO BE SEIZED

This warrant authorizes the use of remote access techniques to search the electronic storage media identified in Attachment A and to seize and copy from the electronic storage media identified in Attachment A the web shells, used by actors to communicate with and distribute files to victim computers to infect them with malware, as evidence and/or instrumentalities of the computer fraud and conspiracy in violation of Title 18, United States Code, Sections 1030(a)(2) (theft from a protected computer), 1030(a)(5)(A) (damage to a protected computer) and 371 (conspiracy). This authorization includes the use of remote access techniques to access the web shells and issue commands through the web shells to the software running on the electronic storage media to delete the web shells themselves.

This warrant does not authorize the seizure of any tangible property. Except as provided above, this warrant does not authorize the seizure or copying of any content from the electronic storage media identified in Attachment A or the alteration of the functionality of the electronic storage media identified in Attachment A.